IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023

A Comparative Study of Machine Learning Techniques for IoT Network Intrusion Detection and Classification

Pooja Hargude[1], Divya Ghate[2], Sacchidanand Linge[3], Rahul Mahajan[4], Dr. Jyoti Deshmukh[5]
Students, Department of Computer Engineering / Information Technology[1,2,3,4]
Professor, Department of Artificial Intelligence[5]
G H Raisoni Institute of Engineering and Technology, Pune, India[1,2,3,4]
G H Raisoni College of Engineering and Management, PUNE, India[5]

Abstract: *As the implementation of Internet of Things (IoT) grows rapidly, cybersecurity remains a major challenge. The detection of attacks in IoT infrastructures is a growing concern, as cyber-attacks can cause failures in the system. Intrusion Detection Systems (IDS) are leading security solutions for IoT networks. Anomaly-based network intrusion detection plays a significant role in protecting networks against various malicious activities. However, the insufficiency of IDS to be deployed for the use of special purpose networks and the class imbalance problem pose significant challenges for IoT security. In this research paper, we present a comparative study of several machine learning models to accurately detect attacks on IoT systems. We also address the problem of imbalanced classes using the Synthetic Minority Over-sampling Technique (SMOTE). Our experimental results demonstrate that the proposed approach can effectively detect and classify various attacks on IoT networks with high accuracy, while addressing the challenges of imbalanced classes*

Keywords: IoT, intrusion detection, classification, Feature Reduction, Multi-Layer Perceptron

REFERENCES

[1] Moustafa, Nour, and Jill Slay. "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)." Military Communications and Information Systems Conference (MilCIS), 2015. IEEE, 2015.
[2] Moustafa, Nour, and Jill Slay. "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 dataset and the comparison with the KDD99 dataset." Information Security J0ournal: A Global Perspective (2016): 1-14.
[3] Moustafa, Nour, et al. "Novel geometric area analysis technique for anomaly detection using trapezoidal area estimation on large-scale networks." IEEE Transactions on Big Data (2017).
[4] Moustafa, Nour, et al. "Big data analytics for intrusion detection system: statistical decision-making using finite dirichlet mixture models." Data Analytics and Decision Support for Cybersecurity. Springer, Cham, 2017. 127-156.
[5] Feature Extraction for Machine Learning-based Intrusion Detection in IoT Networks https://arxiv.org/abs/2108.12722
[6] Supervised Machine Learning Based Network Intrusion Detection System for Internet of Things https://ieeexplore.ieee.org/abstract/document/9225340
[7] Intrusion detection in internet of things using supervised machine learning based on application and transport layer features using UNSW-NB15 data-set https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-021-01893-8
[8] Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study (MQTT-IoT-IDS2020 Dataset) https://www.researchgate.net/publication/348206258_Machine_Learning_Based_IoT_Intrusion_Detection_System_An_MQTT_Case_Study_MQTT-IoT-IDS2020_Dataset

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, June 2023

[9] Internet of Things: A survey on machine learning-based intrusion detectionapproaches https://www.sciencedirect.com/science/article/abs/pii/S1389128618308739
[10] Towards Machine Learning Based IoT Intrusion Detection Service https://link.springer.com/chapter/10.1007/978-3-319-92058-0_56